

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Souichi OKADA et al.

Application No.:

Group Art Unit:

Filed:

Examiner:

For: PERSONAL IDENTIFICATION TERMINAL AND METHOD HAVING SELECTABLE
IDENTIFICATION MEANS OR IDENTIFICATION LEVELS

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). JP 2002-345852

Filed: November 28, 2002

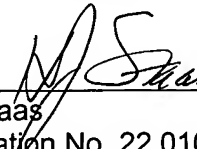
It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date(s) as evidenced by the certified papers attached hereto, in accordance with the
requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Nov. 25, 2003

By: _____


H. J. Staas
Registration No. 22,010

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年11月28日
Date of Application:

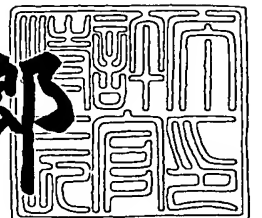
出願番号 特願2002-345852
Application Number:
[ST. 10/C]: [JP 2002-345852]

出願人 富士通株式会社
Applicant(s):

2003年 7月 9日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3055435

【書類名】 特許願

【整理番号】 0295575

【提出日】 平成14年11月28日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明の名称】 個人認証端末、個人認証方法及びコンピュータプログラム

【請求項の数】 10

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 岡田 壮一

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 長谷部 高行

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 蒲田 順

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 林 武彦

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100086933

【弁理士】

【氏名又は名称】 久保 幸雄

【電話番号】 06-6304-1590

【手数料の表示】

【予納台帳番号】 010995

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704487

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 個人認証端末、個人認証方法及びコンピュータプログラム

【特許請求の範囲】

【請求項 1】

複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末であって、

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定することを特徴とする個人認証端末。

【請求項 2】

前記認証手段・レベル指定情報は、電子署名された情報のように、改竄検出可能な形式の情報であることを特徴とする

請求項 1 記載の個人認証端末。

【請求項 3】

前記認証手段・レベル指定情報によって指定された認証手段又は認証レベルが存在しない場合は、あらかじめ定められた認証手段又は認証レベルを使用して個人認証を行うことを特徴とする

請求項 1 記載の個人認証端末。

【請求項 4】

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする

請求項 1 記載の個人認証端末。

【請求項 5】

前記改竄検出可能な形式は、秘密鍵を用いたネットワーク認証プロトコルによるものであることを特徴とする

請求項 4 記載の個人認証端末。

【請求項 6】

認証手段又は認証レベルごとに異なる秘密鍵を使用することを特徴とする

請求項 5 記載の個人認証端末。

【請求項 7】

生体情報による認証手段を使用した場合に、前記認証結果の情報に類似度であるスコアを付加することを特徴とする

請求項 4 記載の個人認証端末。

【請求項 8】

複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末に対して、サーバーから認証要求と共に認証手段・レベル指定情報を送信し、

前記個人認証端末はサーバーから受信した前記認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定し、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする個人認証方法。

【請求項 9】

複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムであって、

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステップと、

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とするコンピュータプログラム。

【請求項 10】

複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、前記コンピュータプログラムが

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステッ

プと、

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複数の認証手段を備え、認証の目的、用途又はシステムのセキュリティレベルに応じて使用する認証手段や認証レベルを選択することができる個人認証端末、個人認証方法及びコンピュータプログラムに関する。

【0002】

【従来の技術】

あらかじめ登録された本人であることをその人の持ち物（IDカード等）、記憶（パスワード等）又は生体情報（指紋等）を用いて認証する個人認証技術は、入退室管理やパーソナルコンピュータのログイン管理等に使用されている。このような個人認証技術には、パスワードやIDカードを用いる比較的簡単なものから指紋、声紋、虹彩等を用いた高度なものまである。また、複数種類（マルチモーダル）の認証手段や認証レベルを備え、それらの組み合わせによってセキュリティの向上を図っているものもある。

【0003】

例えば、特開2000-137844号公報には、勤務時間帯や部屋状況に応じて認証手段（磁気カード、ICカード、指紋等）を変える技術が開示されている。特開2000-145219号公報には、部屋のセキュリティレベルに応じて生体情報による認証の精度（レベル）を設定する技術が開示されている。特開2000-215172号公報には、セキュリティレベルに応じて認証手段（暗証番号、生体情報又はパスワード）を変える技術が開示されている。特開2000-215279号公報には、決済金額に応じて認証手段（暗証番号又は指紋）を変える技術が開示されている。

【0004】

上記のような個人認証装置をサーバーと接続された個人認証端末として使用する形態がある。サーバーに対してサービスの提供を希望するユーザは、個人認証端末を用いてID、暗証番号、生体情報等を入力し、その結果、正規ユーザであることが認証された後に所望のサービスを受けることができる。この場合、生体情報等の個人情報個人情報は個人認証端末側で管理され、サーバーから個人認証装置に対して個人認証の実行を要求し、認証結果が個人認証装置からサーバーに返される。

【0005】

【発明が解決しようとする課題】

複数の認証手段や認証レベルを選択して使用できる個人認証端末において、ユーザが複数の認証手段や認証レベルの中から使用すべき認証手段や認証レベルを選択する必要があるとすれば、ユーザ操作の負担が大きく、使い勝手の悪いものとなる。また、サーバーからの指令により使用すべき認証手段や認証レベルが個人認証端末で指定される場合であっても、認証結果のみが個人認証端末からサーバーに返されるとすれば、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに改竄し、あるいは認証レベルを下げる改竄を行うような不正使用のおそれがある。

【0006】

本発明は、上記のような課題に鑑み、サーバーからの認証要求に応じて個人認証を実行する個人認証端末において、悪意のあるユーザによる不正使用を防止して認証結果の信頼性を高めることを目的とする。

【0007】

【課題を解決するための手段】

本発明による個人認証端末は、複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末であって、サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定することを特徴とする。

【0008】

このような構成によれば、サーバーからの指令によって使用すべき認証手段や

認証レベルが個人認証端末に指定されるので、ユーザ操作の負担が軽くなり、使い勝手が良くなる。

【0009】

好ましくは、前記認証手段・レベル指定情報は、電子署名された情報のように、改竄検出可能な形式の情報である。これにより、個人認証のセキュリティが高くなる。

【0010】

また、前記認証手段・レベル指定情報によって指定された認証手段又は認証レベルが存在しない場合は、あらかじめ定められた（つまりデフォルトの）認証手段又は認証レベルを使用して個人認証を行うことが好ましい。これにより、サーバーからの認証手段又は認証レベルの指定が間違っている場合にも処理を停止することなく対応することができる。

【0011】

更に、本発明による個人認証端末は、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返す。これにより、サーバーは、指定した認証手段又は認証レベルで個人認証が正しく行われたことを確認することができる。換言すると、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに改竄し、あるいは認証レベルを下げる改竄を行うような不正使用を排除することが可能になる。

【0012】

上記の改竄検出可能な形式は、秘密鍵を用いたネットワーク認証プロトコルによるものであることが好ましい。この場合、認証手段又は認証レベルごとに異なる秘密鍵を使用することが更に好ましい。

【0013】

また、本発明による個人認証端末は、生体情報（指紋、声紋、虹彩等）による認証手段を使用した場合に、類似度であるスコア又はそのハッシュ値を前記認証結果の情報に付加することが好ましい。合格（OK）又は不合格（NG）の認証結果だけでなく、スコア又はそのハッシュ値を付加することにより、サーバー側でのきめ細かな対応が可能になる。スコアをそのまま送ってもよいが、そのハッ

シユ値として送ることによりセキュリティが高くなる。

【0014】

本発明による個人認証方法は、複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末に対して、サーバーから認証要求と共に認証手段・レベル指定情報を送信し、前記個人認証端末はサーバーから受信した認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定し、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする。

【0015】

このような個人認証方法によれば、ユーザ操作の負担が軽くなり個人認証端末の使い勝手が良くなると共に、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに変えたり認証レベルを下げたりする改竄行為を排除することが可能になる。

【0016】

本発明によるコンピュータプログラムは、複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムであって、サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステップと、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とする。

【0017】

このようなコンピュータプログラムを処理装置に実行させることにより、ユーザ操作の負担が軽くなり個人認証端末の使い勝手が良くなると共に、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに変えたり認証レベルを下げたりする改竄行為を排除することが可能になる。

【0018】

このようなコンピュータプログラムは、例えばCD-ROMのようなコンピュ

ータ読み取り可能な記憶媒体に記録された状態で供給され、記憶媒体からコンピュータにインストールされ実行される。あるいはネットワークに接続されたサーバー等の他のコンピュータからダウンロードしてインストールし、又は逐次実行することも可能である。

【0019】

【発明の実施の形態】

以下、本発明の実施形態を図面に基づいて説明する。

図1は、本発明の実施形態に係る個人認証端末の構成例を示すブロック図である。この個人認証端末1は、複数種類の認証手段による認証を行うために、複数の（第1～第nの）認証情報入力部11を備えている。認証情報入力部11の具体的な構成としては、暗証番号やパスワードを入力するためのキーボード、生体情報（指紋、声紋、虹彩等）を入力するためのセンサー（センサーチップ、マイクロフォン、CCDカメラ等）のような既存のデバイスを使用することができる。また、個人認証端末1はセキュリティレベルに応じて複数の認証手段や認証レベルの中から1つの認証手段や認証レベルを選択するためのセレクト12及び認証手段・レベル設定部13を備えている。

【0020】

個人認証端末1は更に、CPU（処理装置）14、認証情報格納部15及びプログラム格納部16を備えている。プログラム格納部16に格納されたプログラムにしたがってCPU14が認証（照合）処理を実行する。この際、認証手段・レベル設定部13で設定された認証手段と認証レベルで認証処理が行われる。認証情報格納部15には、認証処理に必要な認証情報、すなわち暗証番号、パスワード、生体情報、PKI（パブリック・キー・インフラストラクチュア）証明書、秘密鍵等が格納されている。

【0021】

なお、認証処理用のプログラムは、例えばCD-ROMのような記憶媒体20に記憶された状態で供給され、読取装置21を介してプログラム格納部（例えば固定ディスク装置）16にインストールされる。後述する通信インターフェイス部17を介してネットワークに接続された他のコンピュータ（サーバー）から認

証処理用のプログラムをダウンロードしてプログラム格納部 16 にインストールしてもよい。

【0022】

また、個人認証端末 1 は、通信インターフェイス部 17 と暗号化・署名処理部 18 を備えている。通信インターフェイス部 17 の働きにより、個人認証端末 1 は各種サービスを提供するサーバー 2 にネットワークを介して接続することができる。サーバー 2 は、例えばパーソナルコンピュータのような端末装置を用いてサービスの提供を求めてきたユーザがあらかじめ登録された正規ユーザであることの認証を行うために、そのユーザがアクセス可能な（例えば端末装置の近くに設置された）個人認証端末 1 に認証要求を送信する。

【0023】

この際、認証要求と共に、認証に使用すべき認証手段や認証レベルを指定するための認証手段・レベル指定情報がサーバー 2 から個人認証端末 1 に送信される。もちろん、認証手段・レベル指定情報が認証要求に含まれる形式で送信されてもよい。この場合、上述のセクタ 12 及び認証手段・レベル設定部 13 は、サーバー 2 から受信した認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定する。

【0024】

また、個人認証端末 1 は、認証結果と共に、実際に認証に使用した認証手段及び認証レベルを特定する使用手段・レベル情報をサーバー 2 に返す（送信する）。これは、サーバー 2 から個人認証端末 1 に送信した認証手段・レベル指定情報で指定された認証手段及び認証レベルで認証が正しく行われたことをサーバー 2 が確認できるようにするためである。この使用手段・レベル情報は、改竄されないように（もし改竄されれば検出できるように）、暗号化・署名処理部 18 によって電子署名が付された後にサーバー 2 へ送信される。必要な場合は、暗号化・署名処理部 18 によって暗号化も行われる。

【0025】

また、個人認証端末 1 において、認証情報として生体情報が用いられた場合は、照合処理の中で計算されるスコア（類似度）又はスコアのハッシュ値（ハッシ

ユ関数で計算された値) が認証結果と共に個人認証端末 1 からサーバー 2 に送信される。スコアをそのまま送るのではなくハッシュ値として送ることにより、暗号化と同様にセキュリティが高まる。

【0026】

更に、個人認証端末 1 は次認証手段判断部 19 を備えている。ある生体情報による認証手段を用いて認証を行ったときのスコアが CPU 14 から次認証手段判断部 19 に通知されると、次認証手段判断部 19 はそのスコアに基づいて次に使用すべき生体情報による認証手段を判断して CPU 14 に通知する。例えば、声紋による認証手段を用いて認証を行った結果、ある程度の類似度 (スコア) が得られたものの OK (合格) レベルに達しなかった場合に、次認証手段判断部 19 が次に使用すべき生体情報による認証手段として指紋による認証手段を CPU 14 に通知する。

【0027】

但し、次認証手段判断部 19 が働くのは、サーバー 2 から送信された認証手段・レベル指定情報で複数の認証手段が指定された場合である。1 つだけの認証手段が指定された場合は次認証手段判断部 19 が働く余地はない。

【0028】

また、ある生体情報による認証手段を用いて認証を行ったときのスコアがあらかじめ定めた最低レベルより低い場合に、CPU 14 は次の認証処理に進むことなく処理を停止する。また、ある生体情報による認証手段を使用して認証を行ったときの類似度であるスコアが完全一致を示している場合は認証結果を不合格 (NG) とする。生体情報による認証では、生体情報の経年変化や外部環境の相違に起因して、認証情報格納部 15 に格納されている照合用の生体情報と入力された生体情報とが完全一致することは極めて稀である。そこで、スコアが完全一致を示している場合は、悪意のある使用者が何らかの方法で入手した照合用の生体情報を入力した可能性が高いので、上記のように認証結果を不合格 (NG) とする。

【0029】

図 2 は、生体情報による認証手段を用いて認証を行う場合の照合処理の例を示

すフローチャートである。先ずステップ#101でスコアSを計算する。つまり、図1の認証情報入力部11から入力された生体情報を認証情報格納部15から読み出した照合用の生体情報と比較して、類似度であるスコアSを計算する。続くステップ#102で、スコアSをあらかじめ定めた最低レベルXminと比較する。スコアSが最低レベルXminより低い場合は、ステップ#107へ移行して処理を停止する。

【0030】

スコアSが最低レベルXminより高い場合は、次のステップ#103でスコアSが100であるか否かをチェックする。この例では、スコアSは0~100の値をとり得る。そして、スコアSが100である場合は、照合用の生体情報と入力された生体情報とが完全一致することを示しているので、ステップ#106に移行して照合結果が不合格(NG)であると判定する。

【0031】

スコアSが100でない場合は、次のステップ#104でスコアSを合否判定値Xrと比較する。スコアSが合否判定値Xrより低い場合はステップ#106に移行して照合結果が不合格(NG)であると判定し、スコアSが合否判定値Xr以上である場合はステップ#105へ移行して照合結果が合格(OK)であると判定する。なお、スコアSの最低レベルXmin及び合否判定値Xrはセキュリティレベルに応じてあらかじめ設定されている。

【0032】

図3は、個人認証端末1をICカード1aとICカードリーダーライタ1bとの組み合わせによって構成した例を示すブロック図である。この構成例では、ICカード1aの側にCPU14、認証情報格納部15、プログラム格納部16及び次認証手段判断部19が備えられ、ICカードリーダーライタ1bの側に認証情報入力部11、セクタ12、認証手段・レベル設定部13、通信インターフェイス部17及び暗号化・署名処理部18が備えられている。また、ICカード1とICカードリーダーライタ1bとの間の通信をおこなうためのインターフェイス23, 24がそれぞれに備えられている。

【0033】

図4は、一定の条件を満たした場合にサーバー側で認証不合格と判断するシステム構成の例を示すブロック図である。この構成例のサーバー2は、個人認証端末1から通信インターフェイス部27を介して受信した認証結果の情報に付加されたスコアのログを格納するスコアログ格納部25と、スコアログ格納部25から読み出したスコア又はそのハッシュ値のログに基づいて、同じスコアが複数回（例えば5回）連続した場合は個人認証端末から受信した認証結果にかかわらず認証不合格（NG）と判定する処理部26とを備えている。生体情報による認証では、生体情報の経年変化や外部環境の変化に起因して、認証の類似度であるスコアが毎回同じであることは極めて稀である。同じスコアが複数回連続した場合は、悪意のあるユーザによって人工的に作られた生体情報が毎回入力された可能性が高い。そこで、このサーバー2では、そのような場合は認証不合格（NG）と判定し、サービスの提供を行わない。

【0034】

図5は、個人認証端末から取得した情報に基づいてサーバーが認証手段・レベル指定情報を変更するシステム構成の例を示すブロック図である。この構成例では、個人認証端末1にRTC・GPS部30が備えられている。RTC（リアルタイムクロック）は、現在の日付及び時刻の情報を生成し出力する。GPS（グローバルポジショニングシステム）は、個人認証端末1の位置情報を生成して出力する。

【0035】

サーバー2から個人認証端末1への認証要求及び認証手段・レベル指定情報の送信に先立って、RTC・GPS部30から出力された現在の日付及び時刻の情報と位置情報を含む認証端末情報が個人認証端末1からサーバー2に送信される。サーバー2の処理部26は、受信した認証端末情報にしたがって、個人認証端末1に送信する認証手段・レベル指定情報を変更する。これにより、サーバー2がサービスの提供を開始する際に、又は認証を行うたびに、認証手段及びレベルが個人認証端末1に設定される。

【0036】

なお、現在の日付及び時刻の情報と位置情報の両方を認証端末情報に含める必

要は必ずしも無く、少なくともいずれか一方が含まれておればよい。また、個人認証端末 1 の装置 ID を認証端末情報に含めてもよい。

【0037】

図 6 は、チャレンジ&レスポンスによる認証手段又は認証レベルの確認方法の例を示す図である。まず、サーバー 2 から個人認証端末 1 に認証手段・レベル指定情報が送信される（ステップ# 201）。認証手段・レベル指定情報を受信した個人認証端末 1 は、認証手段・レベル指定情報にしたがって使用する認証手段又は認証レベルを設定し、生体情報を入力して照合処理を行う（ステップ# 202）。

【0038】

照合処理が完了するとチャレンジコード要求（処理完了通知）が個人認証端末 1 からサーバー 2 に送信される（ステップ# 203）。チャレンジコード要求を受信したサーバー 2 は、乱数をチャレンジコードとして個人認証端末 1 に送信する（ステップ# 204）。チャレンジコードを受信した個人認証端末 1 は、乱数、使用手段・レベル情報、スコア又はそのハッシュ値等を結合して得られるレスポンスコードをサーバー 2 に送信する（返す）（ステップ# 205）。この際、改竄を検出するための PKI 署名を付して送信する。レスポンスコードを受信したサーバー 2 は、指定した認証手段及び認証レベルで認証が行われたことをレスポンスコードから確認することができる。

【0039】

図 7 は、認証結果が合格である場合に、ユーザによる秘密鍵の利用回数を制限するための構成例を示す図である。ステップ# 301 でユーザ（個人認証端末 1 の側）からサーバー 2 にサービス要求が送信されると、サーバー 2 は認証手段・レベル指定情報と共に秘密鍵の利用回数を指定するための利用回数設定情報を個人認証端末 1 に送信する（ステップ# 302）。認証手段・レベル指定情報と利用回数設定情報を受信した個人認証端末 1 は、認証手段・レベル指定情報にしたがって使用する認証手段又は認証レベルを設定し、生体情報を入力して照合処理を行う（ステップ# 303）。照合処理が完了するとチャレンジコード要求（処理完了通知）が個人認証端末 1 からサーバー 2 に送信される（ステップ# 304）。

）。

【0040】

また、認証結果がOK（合格）のときに、個人認証端末1は秘密鍵の利用回数を利用回数カウンタに設定し、秘密鍵が使用されるたびに利用回数カウンタをデクリメントする利用回数管理処理を実行する（ステップ#305）。利用回数カウンタがゼロになれば、秘密鍵の利用ができなくなる。

【0041】

チャレンジコード要求を受信したサーバー2は、乱数からなるチャレンジコードを生成し、個人認証端末1に送信する（ステップ#306）。チャレンジコードを受信した個人認証端末1は、乱数、使用手段・レベル情報、スコア又はそのハッシュ値、そして利用回数情報を結合して得られるレスポンスコードをサーバー2に送信する（返す）（ステップ#307）。この際、改竄を検出するためのPKI署名がレスポンスコードに付される。レスポンスコードを受信したサーバー2は、指定した認証手段及び認証レベルで認証が行われたこと、そして設定した秘密鍵の利用回数が改竄されていないことをレスポンスコードから確認することができる。

【0042】

以上、本発明の実施形態をいくつかの実施例と共に説明したが、本発明は上記実施形態に限定されず種々の形態で実施することが可能である。

（付記1）複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末であって、

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定することを特徴とする個人認証端末。

【0043】

（付記2）前記認証手段・レベル指定情報は、電子署名された情報のように、改竄検出可能な形式の情報であることを特徴とする付記1記載の個人認証端末。

（付記3）前記認証手段・レベル指定情報によって指定された認証手段又は認証レベルが存在しない場合は、あらかじめ定められた認証手段又は認証レベルを

使用して個人認証を行うことを特徴とする付記 1 記載の個人認証端末。

【0044】

(付記 4) 実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする付記 1 記載の個人認証端末。

【0045】

(付記 5) 前記改竄検出可能な形式は、秘密鍵を用いたネットワーク認証プロトコルによるものであることを特徴とする付記 4 記載の個人認証端末。

(付記 6) 認証手段又は認証レベルごとに異なる秘密鍵を使用することを特徴とする付記 5 記載の個人認証端末。

【0046】

(付記 7) 前記認証結果の情報に前記使用手段・レベル情報を付加した情報を暗号化し、又は電子署名を付してサーバーに返すことを特徴とする付記 4 記載の個人認証端末。

【0047】

(付記 8) 生体情報による認証手段を使用した場合に、類似度であるスコア又はそのハッシュ値を前記認証結果の情報に付加することを特徴とする付記 4 記載の個人認証端末。

【0048】

(付記 9) 生体情報による認証手段を使用して認証を行ったときの類似度であるスコアに応じて、次に使用すべき生体情報による認証手段の決定を行うための次認証手段判断部を更に備えていることを特徴とする付記 4 記載の個人認証端末。

【0049】

(付記 10) 生体情報による認証手段を使用して認証を行ったときの類似度であるスコアがあらかじめ定めた最低レベルより低い場合は次の認証処理に進むことなく処理を停止することを特徴とする付記 9 記載の個人認証端末。

【0050】

(付記 11) 生体情報による認証手段を使用して認証を行ったときの類似度で

あるスコアが完全一致を示している場合は認証結果を不合格とすることを特徴とする付記 4 記載の個人認証端末。

【0051】

(付記 12) 前記個人認証端末が、ICカードとICカードリーダーライタとの組み合わせによって構成されていることを特徴とする付記 1 記載の個人認証端末。

【0052】

(付記 13) 付記 8 記載の個人認証端末から受信した認証結果の情報に付加されたスコア又はそのハッシュ値のログを格納するスコアログ格納部と、スコアログ格納部から読み出したスコア又はそのハッシュ値のログに基づいて、同じスコアが複数回連続した場合は個人認証端末から受信した認証結果にかかわらず認証不合格と判断する処理部とを備えていることを特徴とするサーバー。

【0053】

(付記 14) 複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末に対して、サーバーから認証要求と共に認証手段・レベル指定情報を送信し、

前記個人認証端末はサーバーから受信した認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定し、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする個人認証方法。

【0054】

(付記 15) 前記サーバーから前記個人認証端末への認証要求及び認証手段・レベル指定情報の送信に先立って、前記個人認証端末から位置又は現在時刻の情報を含む認証端末情報をサーバーに送信し、サーバーの処理部は、個人認証端末から受信した認証端末情報にしたがって、個人認証端末に送信する認証手段・レベル指定情報を変更することを特徴とする付記 14 記載の個人認証方法。

【0055】

(付記 16) 前記認証要求及び認証手段・レベル指定情報と共に、秘密鍵の利用回数指定情報をサーバーから前記個人認証端末へ送信し、認証結果が合格であ

る場合に、ユーザによる秘密鍵の利用回数を制限することを特徴とする付記 14 記載の個人認証方法。

【0056】

(付記 17) 複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムであって、

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステップと、

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とするコンピュータプログラム。

【0057】

(付記 18) 複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、前記コンピュータプログラムが

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステップと、

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とする記憶媒体。

【0058】

【発明の効果】

以上に説明したように、本発明の個人認証端末、個人認証方法及びコンピュータプログラムによれば、サーバーからの指令によって使用すべき認証手段や認証レベルが個人認証端末に指定されるので、ユーザ操作の負担が軽くなり、個人認証端末の使い勝手が良くなる。また、サーバーは指定した認証手段又は認証レベ

ルで個人認証が正しく行われたことを確認することができるので、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに改竄し、あるいは認証レベルを下げる改竄を行うような不正使用を排除することが可能になる。

【図面の簡単な説明】

【図 1】

本発明の実施形態に係る個人認証端末の構成例を示すブロック図である。

【図 2】

生体情報による認証手段を用いて認証を行う場合の照合処理の例を示すフローチャートである。

【図 3】

個人認証端末を IC カードと IC カードリーダーとの組み合わせによって構成した例を示すブロック図である。

【図 4】

一定の条件を満たした場合にサーバー側で認証不合格と判断するシステム構成の例を示すブロック図である。

【図 5】

個人認証端末から取得した情報に基づいてサーバーが認証手段・レベル指定情報を変更するシステム構成の例を示すブロック図である。

【図 6】

チャレンジ&レスポンスによる認証方法又は認証レベルの確認方法の例を示す図である。

【図 7】

認証結果が合格である場合に、ユーザによる秘密鍵の利用回数を制限するための構成例を示す図である。

【符号の説明】

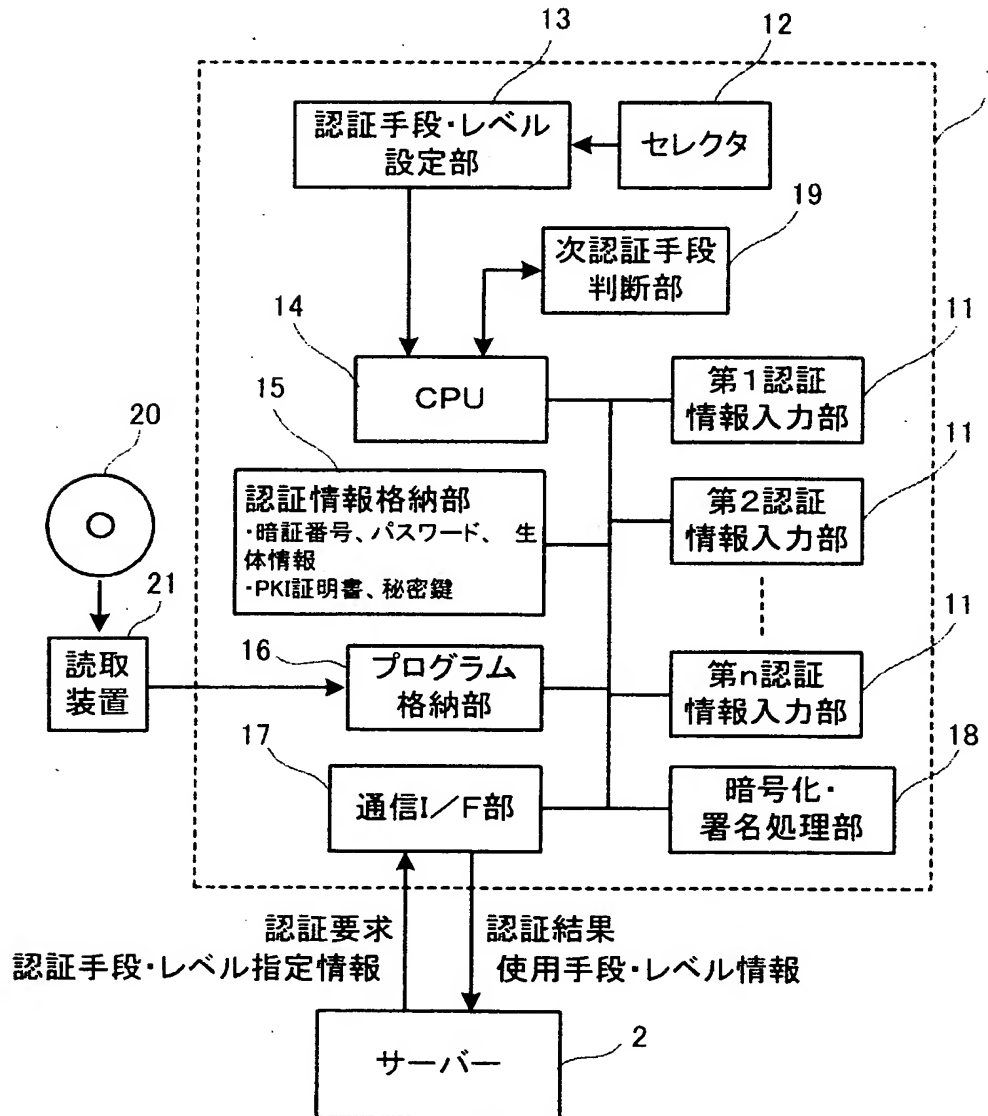
- 1 個人認証端末
- 2 サーバー
- 11 認証情報入力部
- 12 セレクタ

- 1 3 認証手段・レベル設定部
- 1 4 C P U (処理装置)
- 1 5 認証情報格納部
- 1 6 プログラム格納部
- 1 8 暗号化・署名処理部
- 1 9 次認証手段判断部

【書類名】 図面

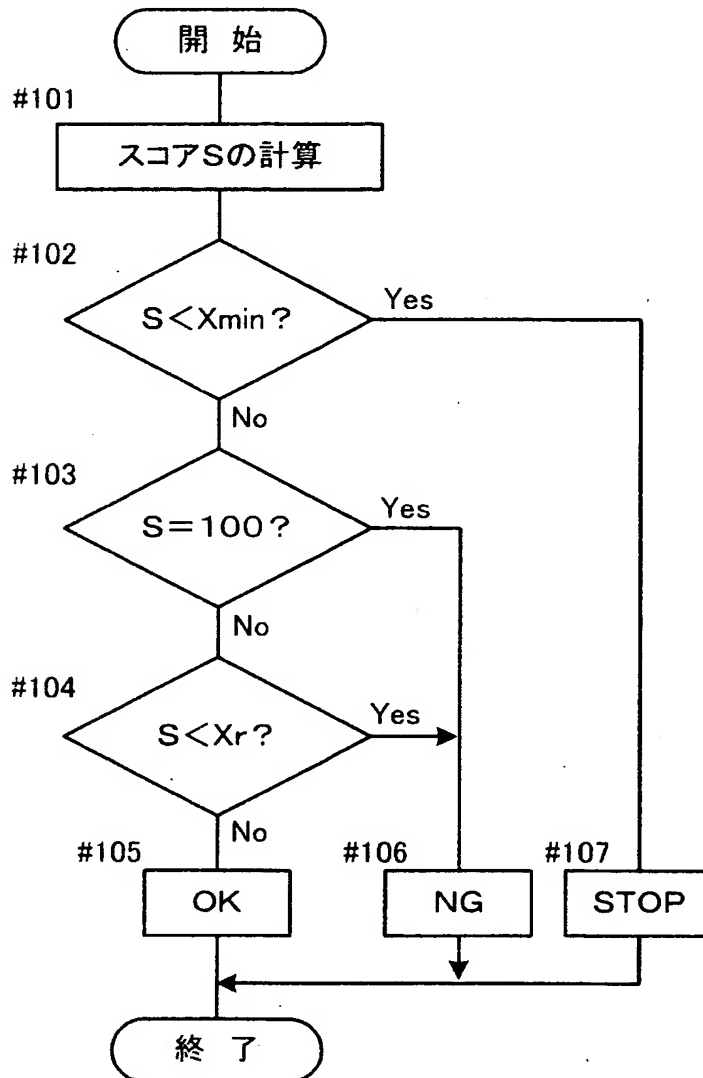
【図 1】

本発明の実施形態に係る個人認証端末の構成例を示すブロック図



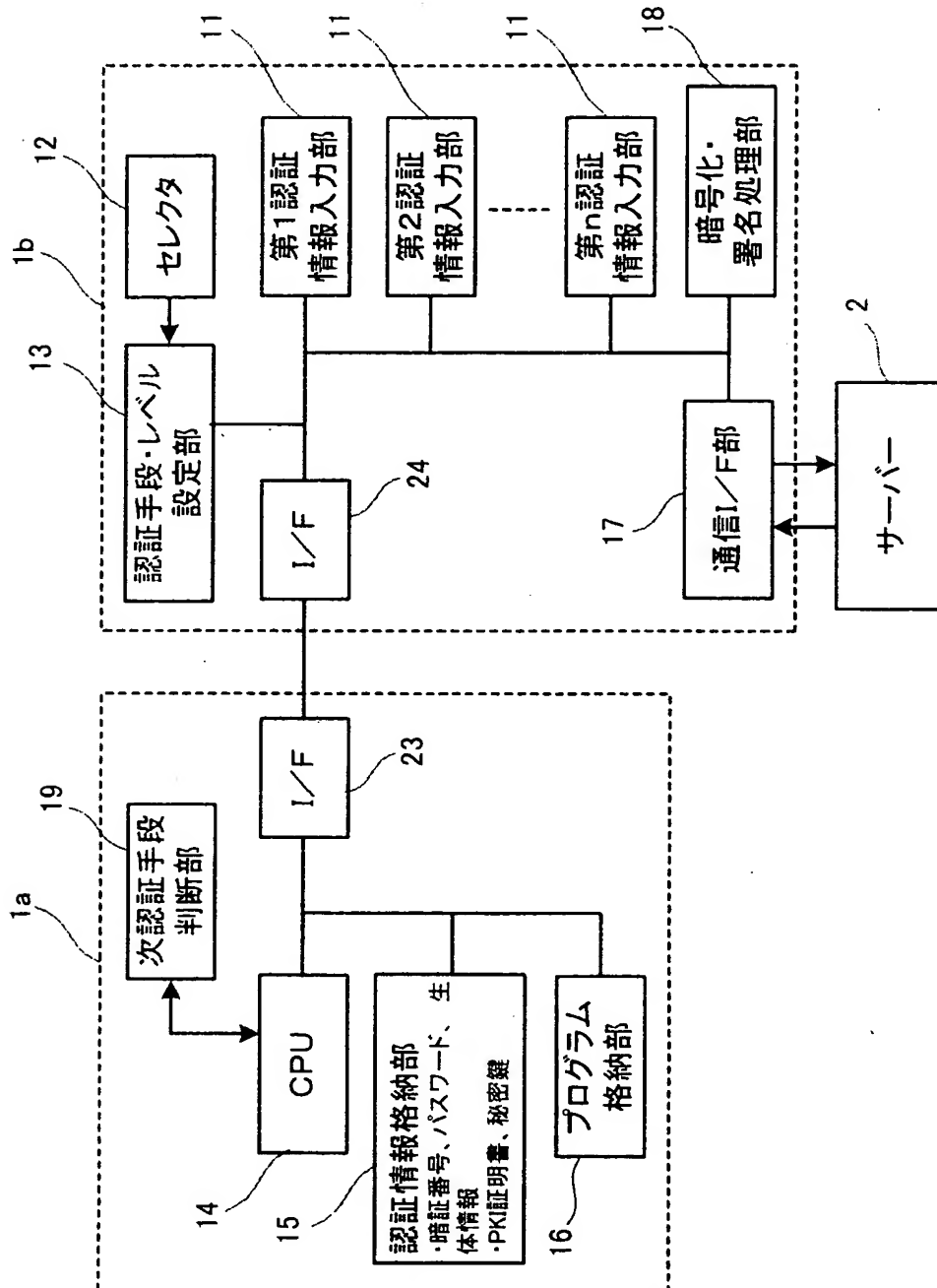
【図 2】

生体情報による認証手段を用いて認証を行う場合の
照合処理の例を示すフローチャート



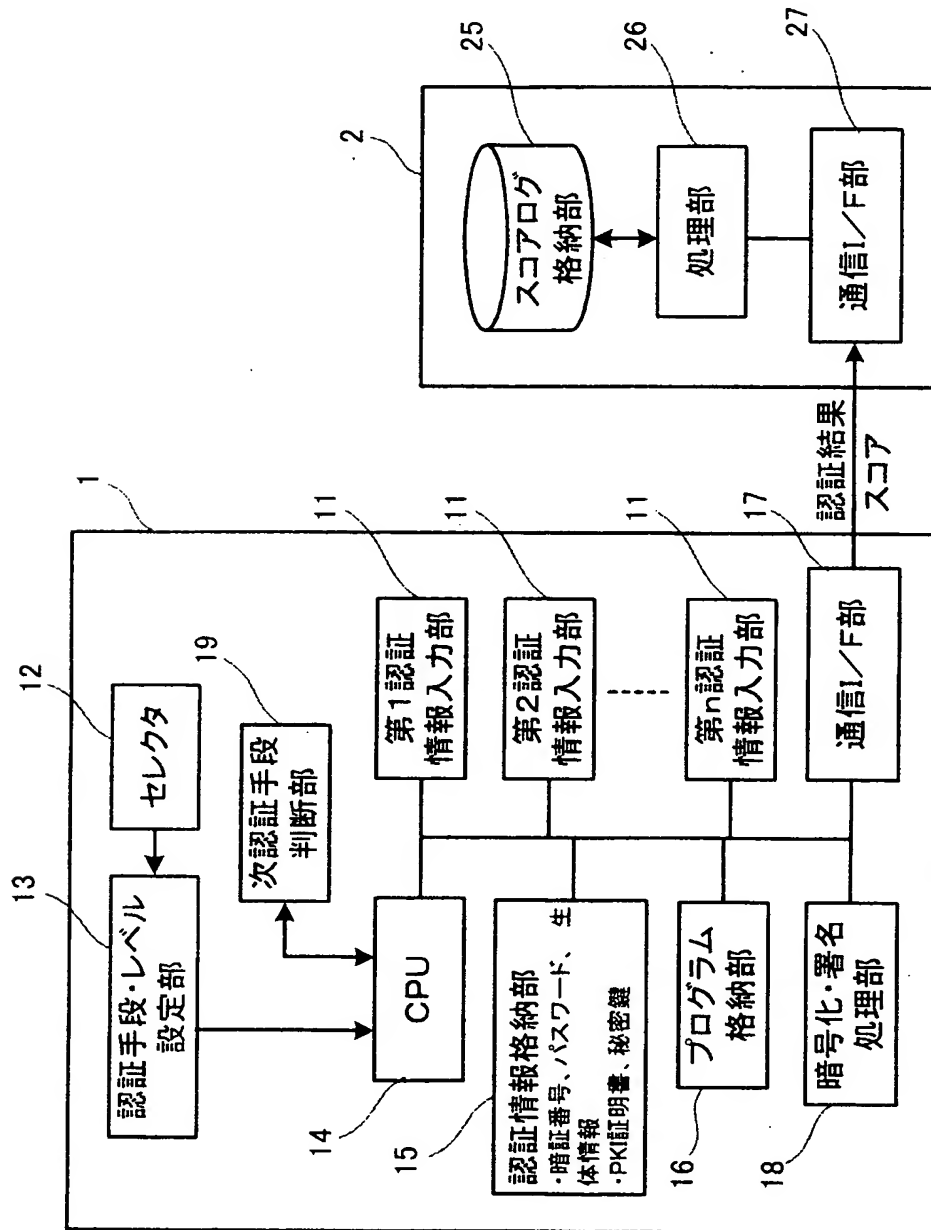
【図 3】

個人認証端末をICカードとICカードリーダーとの組合せによって構成した例を示すブロック図



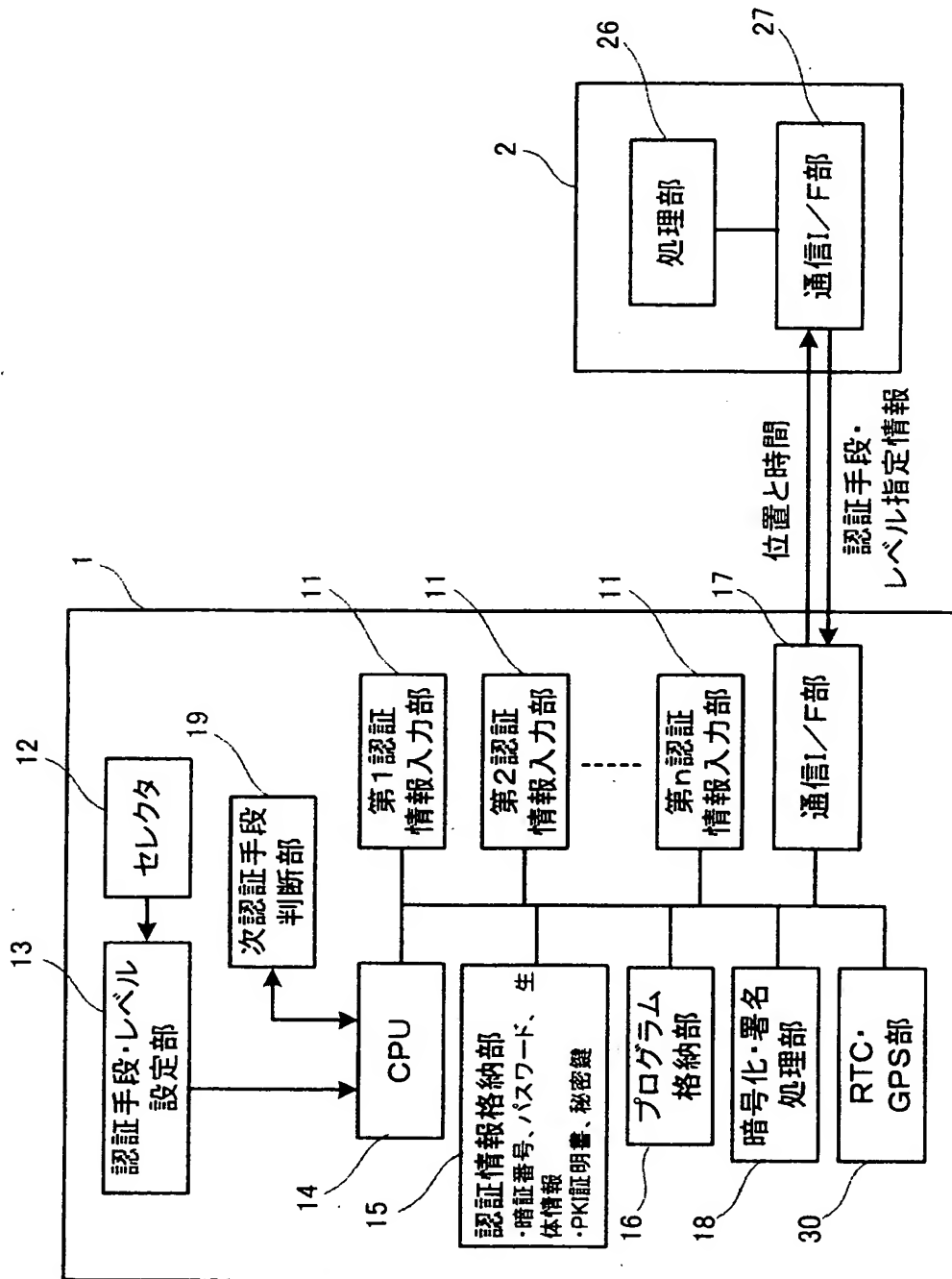
【図 4】

一定の条件を満たした場合にサーバー側で認証不合格と判断するシステム構成の例を示すブロック図



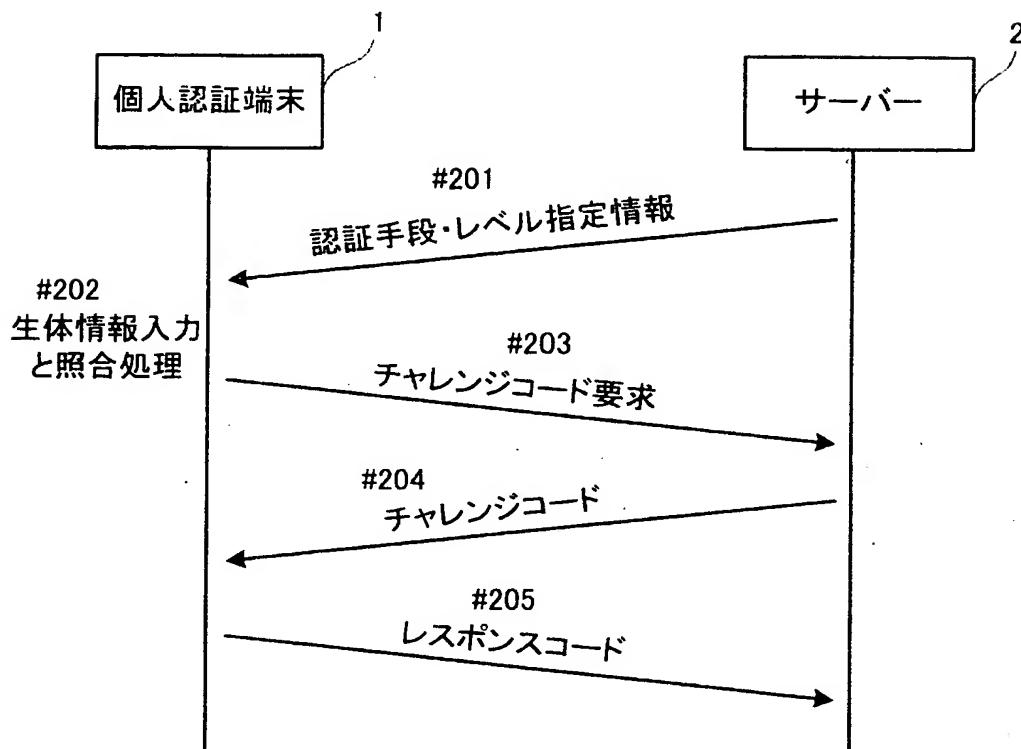
【図 5】

個人認証端末から取得した情報に基づいてサーバーが認証手段・レベル指定情報を変更するシステム構成の例を示すブロック図



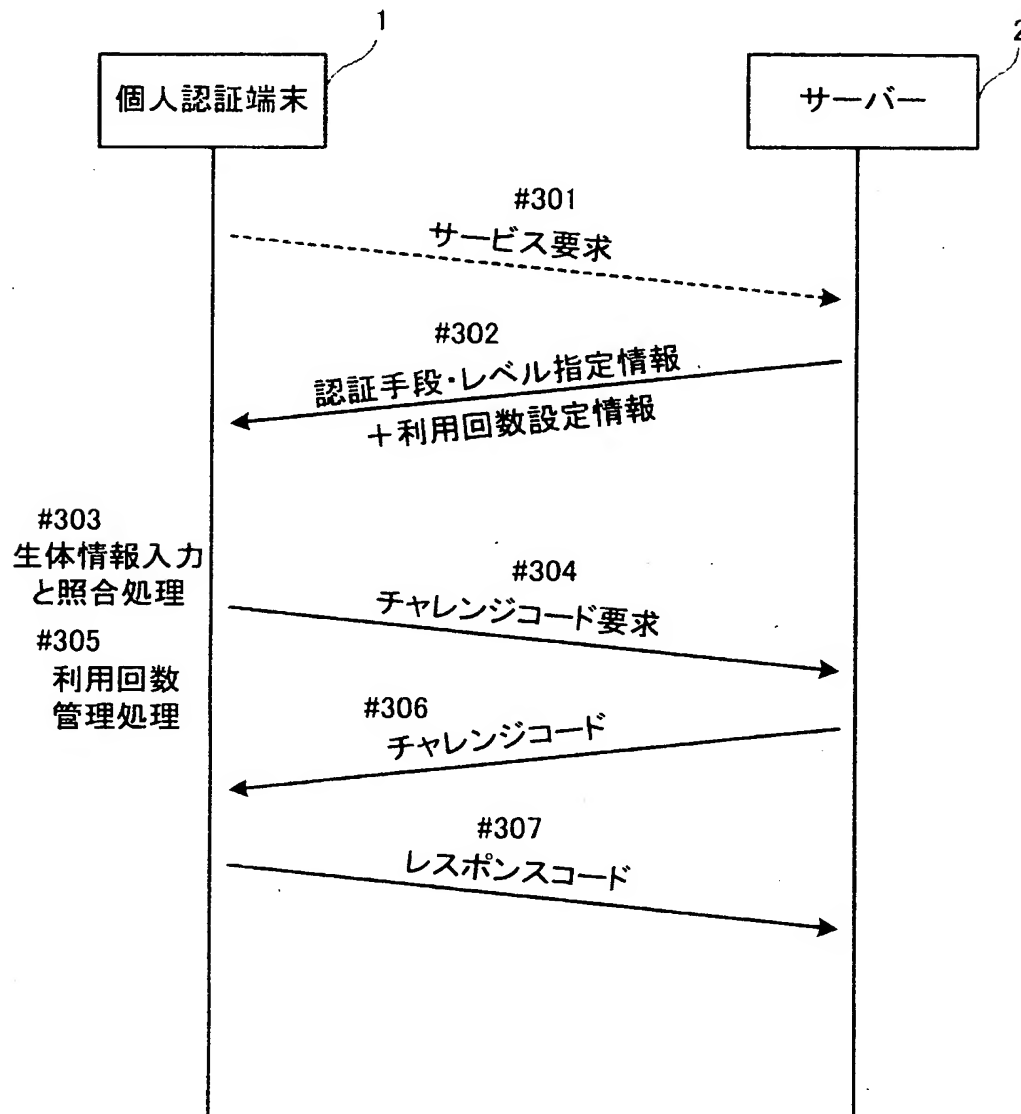
【図 6】

チャレンジ&レスポンスによる認証手段又は認証レベルの確認方法の例を示す図



【図 7】

認証結果が合格である場合に、ユーザによる秘密鍵の
利用回数を制限するための構成例を示す図



【書類名】 要約書

【要約】

【課題】 サーバーからの認証要求に応じて個人認証を実行する個人認証端末において、悪意のあるユーザによる不正使用を防止して認証結果の信頼性を高める。

【解決手段】 複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末において、サーバー 2 から認証要求を受信するたびに、サーバー 2 から受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定する。また、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返す。

【選択図】 図 1

特願 2002-345852

出願人履歴情報

識別番号

[000005223]

1. 変更年月日

1990年 8月24日

[変更理由]

新規登録

住 所

神奈川県川崎市中原区上小田中1015番地

氏 名

富士通株式会社

2. 変更年月日

1996年 3月26日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中4丁目1番1号

氏 名

富士通株式会社